State of Montana Information Security Advisory Council

Minutes
November 17, 2016
11:00 a.m.
Department of Environmental Quality
Room 111

Members Present:

Ron Baldwin CIO/SITSD, Chair
Lynne Pizzini, CISO/SITSD
Joe Frohlich, SITSD
John Burrell, Justice/MATIC Alternate
Margaret Kauska, DOR
Adrian Irish, Uof M
Bryan Costigan, DOJ
John Daugherty, DOC
Kreh Germaine, DNRC
Jim Gietzen, OPI
Joe Chapman, DOJ
Stuart Fuller, DPHHS
Craig Stuart, DMA Alternate

Staff Present:
Wendy Jackson, Marilu Hanson

Guests Present:
Lance Wetzel, Dawn Temple, Brett Dahl, Rebecca Cooper, Daniel Nelson, Amber Godbout, Manuel Soto, Sean Rivera, Tim Kosara

Real-time Communication:
Cheryl Pesta, Christi Mock, Jessica Plunkett, Angie Riley, Michael Jares, John Cross, Erin Stroop, Jerry Marks, Josh Rutledge, Terry Meagher, Anne Kane, Michael Barbere, Suzi Kruger, Zach Day, Cyndie Lockett, Sky Foster

Welcome and Introductions

Ron Baldwin welcomed the council to the November 17, 2016 Montana Information Security Advisory Council (MT-ISAC) meeting. All members and guests were introduced.

Minutes

Margaret Kauska made a motion to approve October 27, 2016 minutes as presented. Kreh Germaine seconded the motion. Motion carried.

Business

Cyber Security Insurance

Brett Dahl gave a presentation on Cyber Security Insurance. Mr. Dahl stated that leading cyber security incidents are phishing, hacking, and malware. Employee actions and mistakes account for 24% of these incidents. It is strongly recommended that employees do not store personal information on their work computers. External theft and vendor thefts are also contributing factors to these incidents. Malware incidents increased 32% from 2014 to 2015. Ransom attacks are on the rise and have spiked from 35,000 to 5,600 infections in March 2016. The state insurance policy does include coverage for ransoms. Laws governing Cyber Security incidents vary between jurisdictions. There is limited president and no case law to define what materially compromises security or confidentiality breaches. If the breach involves more than a thousand residents, there is often a request for credit reporting or credit monitoring. Montana's state insurance offers one year of credit monitoring. Mr. Dahl gave a simplified view of a data breach which includes discovery, evaluation, forensics investigation, legal review. Short term crisis management is conducted by notifying the affected individuals, providing access to credit monitoring, call center assistance, and insurance to protect their assets. Long term consequences may involve class action lawsuits, regulatory fines, penalties and consumer redress, reputational damage and income loss. The cost of responding to breaches for the state of Montana to date is $2.4M. The state of Montana Cyber Security Insurance covers the data breach response costs including but not limited to forensic investigations, mail notification and credit monitoring. This policy also covers business insurance interruption and revenue loss. The state cyber security insurance program has been in place seven years. It is a layer program with a primary insurance layer of $1M to $2M per

occurrence with a deductible of $100,000. This plan covers the entire state, including all agencies and the university system. Administrative safeguards include incident response, vendor management, risk assessments, technical safeguards, two factor authentication and network segmentation to end point sensors. Insurance requirements in contracts for vendors also works as a safeguard against Cyber Security breaches. Breaches should be reported to the insurance provider immediately. The breech should not be made general knowledge until an investigation can be completed. Please report all breeches within 24 hours. Report of incident forms should be completed by the immediate supervisor. Once contacted, the insurance provider will notify carriers, attorneys and the appropriate federal and state officials and law enforcement. This presentation can be found at http://sitsd.mt.gov/Governance/ISAC.

Mr. Baldwin requested that Mr. Dahl provide examples of vendor contract language.
Action Item: Mr. Dahl will provide SITSD with vendor contact language.

Q: Mr. Baldwin: What are the technical requirements for what they consider to be segregation of systems?
A: Stuart Fuller: Technical requirements for segregation of systems are not clear. It is up to the organization to define contract language. The national Institute of Science and technology (NIST) gives the base guidance and it is usually as organizationally defined rules. There is some specific contract language from the SSA and CMS on security requirements.

MT-ISAC Topics of Discussion
Google Documents, Exceptions
Lynne Pizzini spoke to the council about google documents and exception requests for access. There are 2,272 users out of 17,000 that have access to google documents. In the past, if more than 50% of users have exceptions, the filter would be removed. Ms. Pizzini recommended that the filter be kept in place and exceptions be issued for users that need access to google documents. Ms. Pizzini confirmed that this filter is in place to prevent data from going out externally. There is research being conducted on Data Loss Prevention (DLP) that is looking at putting that on Websense, the web filtering product. Ms. Pizzini requested time to research this matter further and readdress the topic at a later date.

Q: Mr. Fuller: Is there an increased hacking risk with google documents?
A: Ms. Pizzini: According to our research google documents is similar other document storage places. It does have security requirements.

Disposal of Media Storage, Destruction Process
Ms. Pizzini discussed the disposal and destruction of media storage. MT-ISAC is exploring an enterprise solution for media storage disposal and destruction.
Action Item: Ms. Pizzini will provide an update on Media Storage Disposal and Destruction at the January 4, 2017 MT-ISAC meeting.

Server Antivirus Update
Joe Frohlich stated that a contract is expected to be be signed for Linux servers by the end of November, 2016.

IT Conference Security Tracks
Mr. Frohlich reminded the council that there will be several presentations related to It Security at the IT Conference the week of December 12, 2016. The agenda for the IT Conference can be found at itconference.mt.gov.

Upcoming Legislative Session
Mr. Baldwin gave a brief review of the upcoming legislative session. There is no House Bill 10 this year. By managing SITSD's biennial budget and working capital carefully there may be potential avenues for funding of IT security initiatives. Volume 10 has been published alongside the governor's executive budget. This report has the potential to generate discussion concerning information technology at an enterprise level for the state and how IT funds are utilized.

Workgroup Updates
Assessment Workgroup
Policy Assessment Tool Update

Mr. Frohlich updated the council on the policy assessment tool. Mr. Frohlich recommended that the council adopt the nationwide cyber security review as the policy assessment tool. The US Department of Homeland Security is partnered with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to develop this tool. There are a hundred and twelve questions which cover the core components of the cyber security and privacy. This assessment takes approximately two hours to complete. The council has approved the use of the National Cyber Security Review (NCSR) as a tool to provide a yearly state information security assessment. This assessment will outline program success and address shortcomings. This tool meets the objective of implementing a statewide standardization information security program assessment in measurements for departments in the state. This tool is managed by MS-ISAC. There is no sensitive information involved in this assessment. This year's NCSR opened on November 4th and will close December 31st. If approved, the first report by agencies would be due December 3, 2017. The MT-ISAC assessment team will provide a guide to assist agencies in answering questions. Individuals interested in trialing the NCSR tool should contact Mr. Frohlich at jfrohlich@mt.gov.

Q: Kreh Germaine: Since there is no sensitive information in the assessment, where does that fall in relation of protection for sunshine laws? Is that still something that falls under protection or is that public information?
A: Ms. Lynne: NCSR is on a secured site. There is also a nondisclosure agreement with MS-ISAC that covers the NCSR.
Q: Mr. Germaine: Is our legal office confident that they would be able to defend the nondisclosure agreement if a request for information came in? Would that nondisclosure agreement still apply, given that the information provided is just that general assessment?
A: Ms. Pizzini: This is the question we need to ask our legal office.
Action Item: Ms. Pizzini will ask the legal team if the nondisclosure agreement would apply to information provided through the policy assessment tool.

Best Practices / Tools Workgroup Update
Ms. Pizzini gave a report on the Acceptable Use / Best Practices Workgroup. The Acceptable Use document was submitted for the council to review. There have been several comments and questions related to this document. This document has been revised to include information concerning the discrepancy between the service desk and the help desk. Information will be added regarding the sensitive information on portable devices. Verbiage will also be incorporated into the best practices user addressing user responsibility. The current best practices document addresses the responsibilities of the user and provides recommended forms. This form is being signed by all new employees who use the Summer system in Taleo. It is automatically sent to users. This document will be incorporated into the Acceptable Use document. It will also be maintained in the Summer system as a document that all new employees will be required to sign before they come to work for the state. There is a slight change that needs to be made to the wording but will not alter the documents' content. Ms. Pizzini confirmed that all policies are available in the mom.mt.gov Montana Operations Manual.
Action Item: These changes will be incorporated into the Acceptable Use document. MT-ISAC will be informed when these changes are complete. There will be a vote to approve this document in the January 11, 2017 MT-ISAC meeting.

Mr. Germaine commented that the requirement to resign this agreement every year creates an undue burden on state employees.
Ms. Pizzini stated that the annual signing is a requirement in the state security policy.
Mr. Frohlich commented that this document could be signed electronically to reduce excess paperwork.
Mr. Germaine agreed that a digital format would simplify the annual signing process.
Ms. Kauska offered the assistance of Department of Revenue (DOR) staff to help automate the annual signing process.

Q: Mr. Frohlich: Is there a way to add agency specific modules to Taleo? It would be helpful to be able to store all documents that require signatures in one location.
Action Item: Ms. Pizzini will check to see if it is possible to add agency specific modules to Taleo.

Q: Jim Gietzen: Is the Acceptable Use document for end users or is this for IT professionals?
A: Ms. Pizzini: It was designed for end users.

Mr. Gietzen suggested that definitions be added to the Acceptable Use document to clarify what is meant by IT resources. The document also states that work related files shall be stored on state network. This is

inaccurate as many agencies utilize cloud services to store information.

Action Item: Ms. Pizzini will correct this verbiage to reflect current policy and have the document reviewed by non-personnel to check for clarity.

Mr. Germaine suggested that the wording in the Acceptable Use document be modified to reflect that SITSD will is not actively monitoring the activities of individual users.
Action Item: Mr. Germaine will provide Ms. Pizzini with recommended wording to address this concern. The revised wording will be incorporated into the Acceptable Use document and sent through legal review.

Data Loss Prevention
Mr. Frohlich updated the council on Data Loss Prevention. DLP will be implemented for Office 0365 which will include SharePoint online and OneDrive on November 21, 2016. The DPL template will flag emails or documents containing nine or less social security numbers. An email will be sent stating that there is sensitive information contained in the document or email. Documents containing nine or less social security numbers can still be posted on SharePoint. This template will block other users from viewing documents containing more than nine social security numbers on both SharePoint and OneDrive. This template uses an algorithm to identify sensitive information and will not flag a nine-digit code unless it recognizes as a social security or credit card number. DLP for Exchange will be turned on in audit mode November 21, 2016. This template will send a tool tip alerting users that the document or email they are sending contains sensitive information. Once fully implemented, DLP will function the same for Exchange as SharePoint and OneDrive. The tool tip will contain a link to a website containing information as to why your email is being blocked. DLP in audit mode will not block information from being sent. Notifications will be made in NMG meetings as to the exact date of when DLP will be turned on in audit mode for Exchange.

Joe Chapman expressed concerns that this template needs to be thoroughly tested prior to implementation to avoid disruption of business.
Ms. Pizzini stated that MT-ISAC utilized the Best Practices workgroup to solicit input and testing from system users. DPL was then reviewed by MT-ISAC, NMG, and ITMC to request input and user testing of the system prior to full implementation. These discussions have been documented in the meeting minutes and a change request was sent out.

Q: Mr. Germaine: What is the process for reviewing and improving DLP if there are major business disruptions due to implementation?
A: Ms. Pizzini: in that case, DLP would be sent back to the workgroup for review and revision.

Mr. Chapman suggested the workgroup hold an official vote to approve the DLP template to formalize the process.
Ms. Pizzini stated that the DLP process will follow the standard change process and a communication will be sent out from the service desk.

Mr. Gietzen suggested that there be a centralized location and formal communications for information concerning decisions and actions taken in board and council meetings.

Mr. Baldwin stated that all decisions and actions taken in board and council meetings can be found in the meeting minutes. A change control could be instituted, similar to the process recently incorporated in NMG, to formalize and document awareness of decisions.
Action Item: Mr. Baldwin will discuss the incorporation of a change control board with the ITMC executive council.

Situational Awareness Workgroup
Outreach Public Safety Workgroup Update
John Burrell stated that the workgroup has been suspended until January. The workgroup has held discussions on what the information sharing with the private sector might look like. There will be further updates provided to MT-ISAC once the workgroup resumes in January, 2017.

Current Threats/Tabletop Exercise

Sean Rivera spoke to the council concerning Current Threats. The largest potential data breach on record has occurred with the exposure and data breach of 412M email addresses, passwords, and IP addresses of the members a network called Friend Finder or Adult Friend Finder. Some of the issues connected with breeches of this nature include passwords being stored in plain text, or using deprecated salting methods which is very easily hacked. A large number of Hotmail accounts along with 70,000 US military email accounts and 56,000 US government accounts were also breached during this event. There is a new US Office of Personal Management (OPM) phishing scam that is connected to the Locky Ransomware campaign where entities are required to pay to unlock their systems. This phishing scam includes a poorly written email warning users about suspicious bank activity. There has been ransomware protection added to the Windows 10 anniversary edition which was released in August 2016. This protection makes users 58% less likely to encounter a ransomware infection. Mr. Rivera suggested state users migrate to Windows 10 as quickly as possible. There was a DYN distributed Denial-of-Service attack on October 21st, 2016 which caused issues with latency and dimness. This attack affected sites like Twitter, Netflix, Red Et, and CNN. If agencies wish to conduct table top exercises, Mr. Rivera and his team can provide scenarios for agencies to conduct regular reviews. Interested parties should contact Mr. Rivera at srivera@mt.gov or James Zito at jzito@mt.gov.

Open Forum
Future Agenda Items
Mr. Baldwin stated that future MT-ISAC agenda topics will include discussion of governance, Taleo updates and Data Loss Prevention updates.
Mr. Fuller suggested that the power outage on November 17, 2016 be a topic of discussion on the next MT-ISAC agenda.

Public Comment
None

Adjournment
Next Meeting
January 11, 2017
1:00 PM to 3:00 PM
Cogswell Room 151

Adjourn
The meeting was adjourned at 1:02 PM